IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: **DELLMO ET AL.**	)
	) Examiner: J. Pan
Serial No. **10/806,668**	)
Confirmation No. **1171**	) Art Unit: 2135
Filing Date: **March 23, 2004**	)
For: **MODULAR CRYPTOGRAPHIC DEVICE PROVIDING STATUS DETERMINING FEATURES AND RELATED METHODS**	)

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Responsive to the final Official Action of October 20, 2008, and in connection with the Notice of Appeal filed concurrently herewith, please consider the remarks set out below.

I. The Claims Are Patentable

Independent Claims 1, 11, 21, 25, and 29 are rejected over Dhir et al. in view of Cheng in further view of Klein. Applicants submit that even a selective combination of the prior art fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing.

Dhir et al. is directed to a programmable integrated circuit, namely a field programmable gate array (FPGA), that can be used to handle different wireless local area network (WLAN) communication specifications. The integrated circuit includes a transceiver coupled to programmable gates, memory coupled to the programmable gates for storing instructions for

programming a first portion of the programmable gates with a selected one of a first type of a medium access layer and a second type of a medium access layer. The first type of the medium access layer is different from the second type of medium access layer, though both the first type of the medium access layer and the second type of the medium access layer are compatible with the transceiver. The memory is configured for storing instructions for programming a second portion of the programmable gates as a baseband controller. (See, e.g., Col. 2, lines 14-49 of Dhir et al.).

The Examiner correctly acknowledges that Dhir et al. fails to teach a cryptographic module and a communications module that are removably coupled to one another, a LAN interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices, and a cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner then turned to Cheng for one of these critical deficiencies. Cheng is directed to an add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks. The add-on card includes an access control circuit, volatile and non-volatile memory, a wireless transmission module, and a network connection module. The network connection module has both an antenna for communicating with a wireless network, and a standard network cable port for connecting to a wired network. (See, e.g., paragraphs 0009-0010 of Cheng).

The Examiner still further recognized that even a selective combination of Dhir et al. and Cheng fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner turned to Klein for this critical deficiency. Klein is directed to data security for digital data storage. More particularly, Klein discloses using a key to encrypt data between a data source and a data storage device.

Applicants submit that the Examiner mischaracterized Klein, as Klein fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner first turned to Col. 8, lines 61-64 of Klein, which disclose, "The computing apparatus of claim 1, wherein said bus-to-bus bridge additionally comprises a circuit for selectively disabling said logic circuit from encrypting said digital data." As recited in independent Claim 1 of Klein, "a configuration register in the bus-to-bus bridge is adapted to selectively enable and disable encryption depending on the target device that is to receive the data that is transmitted via the bus-to-bus bridge." Col. 6, lines 23-41 of Klein describe the configuration register and provides an example where the user may want to encrypt some, but not all, data stored onto a floppy disk. Indeed, the passage cited by the Examiner has nothing to do with tampering, but merely controlling which selection of data is to be encrypted.

The Examiner further contended that Col. 7, lines 44-45 of Klein disclose a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. Instead, Col. 7, lines 44-45 of Klein disclose, "Tampering with the logic circuit 50 may also result in incorrect key generation." Nowhere else in Klein is tampering mentioned. Indeed, Klein only mentions that tampering with the logic circuit, and not a first housing, may result in incorrect key generation, and not a disablement. Indeed, the Examiner is merely turning to disjoint passages in Klein in an attempt to support his contention that Klein discloses the claimed invention. Applicants further submit that a person having ordinary skill in the art would not recognize the mere recitations of "tampering" and "selective disablement" in the context of encrypting some, but not all, data, as teaching a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing. Accordingly, Klein fails to disclose a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing, as recited in the independent claims.

Applicants further submit that the Examiner's combination of Dhir et al., Cheng, and Klein is improper, as a person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. and Klein to arrive at the claimed invention. More particularly, Dhir et al. is directed to a programmable logic device for a WLAN. The communications module and the cryptographic module are purposely on a single circuit board (330), as illustrated in Fig. 8 of Dhir et al. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single circuit board.

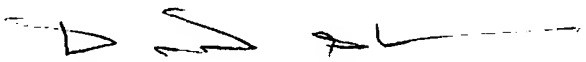
Moreover, using Cheng as a motivation to modify Dhir et al. would result in arbitrarily dividing the circuitry of Dhir et al. between the antenna 336 and the WLAN transceiver 301, the antenna being outside the circuit board and downstream from both the communications and cryptographic modules. This is because Cheng discloses removably coupling the communications modules to a connector portion, including a physical connector and antenna. Accordingly, even if there was some proper motivation to combine Dhir et al. and Cheng, the claimed invention is not produced because the removable coupling is not between the communications module and the cryptographic module.

Still further, one of ordinary skill in the art would not turn to the data security system for digital storage to combine with the programmable integrated circuit from Dhir et al. and the add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks from Cheng. In other words, the Examiner is attempting to combine an FPGA for a wireless LAN with a PCMCIA network add-on card and a system for providing security for digital data stored on data storage media. Applicants submit that the Examiner is merely combining disjoint pieces of the prior art in an attempt to arrive at the claimed invention, and that the Examiner's combination of references is improper.

Accordingly, it is submitted that independent Claims 1, 11, 21, 25, and 29 are patentable

over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407/841-2330
Attorneys for Applicants